UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff, v. JOHN DOES 1-100, Defendants.	CASE NO. C17-1880 RSM ORDER DENYING PLAINTIFF'S MOTION TO EXPEDITE DISCOVERY

I. INTRODUCTION

Plaintiff alleges that Defendants are engaged in a complex internet "phishing" scheme to unlawfully obtain account access credentials from Microsoft customers. Dkt. #1. Specifically, Plaintiff alleges that Defendants transmit misleading and deceptive "Account Update" emails to Microsoft customers in an effort to fraudulently obtain user names and passcodes for customers' Microsoft Accounts ("MSAs"). *Id.* Plaintiff now seeks permission to take expedited discovery from GoDaddy.com, LLC, A2 Hosting, Inc., NameCheap, Inc., Google, Inc. and Cloudflare, Inc. Dkt. #4 at Section D., ¶ 14a.-e. As further discussed below, Plaintiff has failed to meet the standard required for expedited discovery at this time. As a result, the Court does not find that good cause exists to allow Microsoft to engage in expedited, preliminary discovery.

II. BACKGROUND[1]

Plaintiff, Microsoft, is a Washington corporation with its principal place of business in Redmond, Washington. Dkt. #1 at ¶ 3. Microsoft develops, markets, distributes, and licenses computer software, among other products and services. *Id.* One of these products is Office 365. According to Microsoft, Office 365 signifies a revolutionary change in the way that it delivers its software to consumers. *Id.* at ¶ 9. Previously, Microsoft licensed its popular Office suite of productivity products – which includes Word, Excel, PowerPoint, Outlook, OneNote, Publisher, and Access, among others – to computer users who installed and stored the software on their computer systems locally. *Id.* With Office 365, Microsoft Office is available on a subscription basis that uses and leverages Microsoft's Azure cloud technology. Now, customers purchase a subscription to Office 365 that provides access to both cloud and locally-stored versions of the software. *Id.* at ¶ 10. This allows customers to receive instant access to the latest versions of each program, and use the programs across multiple devices (such as laptops, phones, tablets, etc.). An Office 365 subscription also comes with cloud storage. *Id.*

Office 365 can be licensed for consumer or personal use (through the Personal, Home or Student products) or for commercial use (through the Business or Enterprise products). *Id.* at ¶ 12. Using either type of Office 365 service requires the establishment of online accounts. *Id.* For the consumer use products, a user must create or use an existing MSA consisting of an email address and password. *Id.* at ¶ 13. The commercial Office 365 products are created for organizations, which are identified as Tenants. *Id.* at ¶ 14. User accounts within a Tenant are set-up in one of two ways that take advantage of Microsoft's Azure Active Directory product –

[1] The following background is taken from Plaintiff's Complaint and the Declaration of Pierre ("Peter") Anaman filed in support of Plaintiff's Motion for Expedited Discovery. Dkts. #1 and #4.

a cloud-based directory and identity management system. Dkt. #1 at ¶ 14. First, the Administrator of the Tenant can set up individual Office 365 Commercial User Accounts. Second, the Administrator can create several Accounts in bulk. *Id.*

As noted above, Plaintiff alleges that Defendants have engaged in a phishing scam targeting Office 365 users. "Phishing" is a broad term that can encompass many different activities. Dkt. #4 at ¶ 3. The most well-known phishing schemes fall under the umbrella of social engineering attacks. Generally, these schemes involve an individual or group creating spoofed emails that purport to be from legitimate businesses, agencies or individuals. *Id.* These emails are designed to lead the recipient to fake websites that trick users into divulging sensitive information, such as financial account data, login credentials and other personally identifiable information. *Id.* at ¶ 4. The people behind the fake websites harvest personal information and use it to access peoples' accounts for their own illicit gain. *Id.* They may also sell the personal information to others. They may also use the initial email or fake website to infect users' computers with malware. *Id.* at ¶ 5. This malware can further expose unsuspecting victims' personal information, for example, by searching the computer for sensitive files, or even monitoring key strokes to harvest personally identifiable information entered into websites. Malicious software also allows the criminals to hijack a computer or network to propagate further attacks. *Id.*

Microsoft asserts that it goes to great lengths to protect customer's online accounts. *Id.* at ¶ 7. In particular, Microsoft points to the fact that it engineered Office 365 to prevent spam, viruses and malware from even reaching Office 365 users. *Id.* For example, Microsoft built multiple spam filters into Office 365 mail accounts so customers' email addresses are protected from the moment the first message is received. Microsoft uses three anti-malware engines to

detect potentially dangerous software that may be sent to users. Dkt. #4 at ¶ 7. Microsoft also offers Office 365 Advanced Threat Protection, which helps protect a user's mailbox against new, sophisticated attacks in real time. *Id.* In addition to stopping phishing attempts before they reach users, Microsoft also investigates, identifies and stops the criminals behind malicious attacks. *Id.*

Prior to filing this lawsuit, Microsoft explains that it used various investigative techniques to uncover Defendants' alleged phishing scheme. *Id.* at ¶ 8. According to Microsoft's investigator, Pierre Anaman, Defendants' scheme starts by sending unsolicited bulk email purporting to be from the "The account team," to their potential victims. *Id.* at ¶ 9. The emails' subject line is "Email 365 Termination Last Notice, Update Today." *Id.* The body of the email states: "we've detected your Email account is due for upgrade today. To help keep you Active, we've required an Account Update." *Id.* The email goes on to state "Validate today to avoid instant email closure" and then provides a button for the user to click on. *Id.* The language and formatting of the email is designed to appear as if the email came from Microsoft. By clicking on the "Validate Account Now" button in the Phishing Email, the user is brought to a page that purports to be a logon page to Office 365 (the "Phishing Page"). *Id*. at ¶ 10. This page uses Microsoft's trademarks and other designs to create the appearance of being a legitimate Microsoft webpage when in reality it is a counterfeit of Microsoft's Office 365 logon page. *Id.*

The Phishing Page is located on a website that uses the domain name defendworld.eu. *Id.* at ¶ 11. Based on a search of public records relating to that domain, the registrar is GoDaddy.com, LLC. *Id.* The registrant of the domain is listed as "Nuno Pires." *Id.* Microsoft identified and verified that the IP Address used to host defenworld.eu was IP 209.124.68.118, which is administered by a third-party web hosting company, A2 Hosting, Inc. ("A2 Hosting"). *Id.* The content from the Phishing Page, therefore, is hosted on a server that belongs to and is

controlled by A2 Hosting. Dkt. #4 at ¶ 11. However, Microsoft could not (and cannot) determine the identity of the persons behind the website from public records. *Id.*

After entering login credentials, sometimes a Pop-Up dialogue box presents to the user ("Pop-Up"). *Id.* at ¶ 12. This Pop-Up purported to be a safety alert from Microsoft: "Windows Defender Alert: Zeus Virus Detected In Your Computer." *Id.* The Pop-Up provides a number for the user to call at "Microsoft's Technical Department." *Id.* This Pop-Up is not affiliated with Microsoft, is not advertising authorized Microsoft services, and instead, is part of Defendants' scheme to defraud Microsoft's customers. *Id.* The Pop-Up is hosted on a website that uses the domain azure1.us. Based on a search of public records relating to this domain, the registrar is NameCheap, Inc. The registrant of the domain is listed as "Anatoliu Golovin," and the registrant's email address is listed as opel73rus@gmail.com. *Id.* The domain azure1.us is hosted on a server owned or controlled by Cloudflare, Inc. *Id.*

III. DISCUSSION

This Court may authorize early discovery before the Rule 26(f) conference for the parties' and witnesses' convenience and in the interests of justice. Fed. R. Civ. P. 26(d). Courts within the Ninth Circuit generally consider whether a plaintiff has shown "good cause" for such early discovery. *See, e.g., Yokohama Tire Crop. v. Dealers Tire Supply, Inc.*, 202 F.R.D. 612, 613-14 (D. Ariz. 2001) (collecting cases and standards). When the identities of defendants are not known before a Complaint is filed, a plaintiff "should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds." *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). In evaluating whether a plaintiff establishes good cause to learn the identity of John Doe defendants through early discovery, courts examine whether the plaintiff

(1) identifies the John Doe defendant with sufficient specificity that the Court can determine that the defendant is a real person who can be sued in federal court, (2) recounts the steps taken to locate and identify the defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) proves that the discovery is likely to lead to identifying information that will permit service of process. *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999).

Here, Plaintiff has not yet established good cause to engage in early discovery to identify the John Doe Defendants. While Plaintiff has associated the John Doe Defendants with specific phishing activities, and has been able to trace those activities as originating from a certain IP address and servers, it has not alleged that the IP address and/or any of the hosting companies or servers are located in this judicial District. *See* Dkt. #4 at ¶ ¶ 11-13. Thus, the Court cannot determine the likelihood that any of the John Doe Defendants could be sued in this Court. Further, Plaintiff fails to attach any proposed subpoenas to its motion, or describe what discovery it will seek from each of the entities it plans to serve. Thus, the Court is unable to determine whether discovery is likely to lead to identifying information that will permit service of process on the John Doe Defendants. For these reasons, the motion will be denied at this time.

IV. CONCLUSION

Having reviewed Plaintiff's motion and the remainder of the record, the Court hereby ORDERS:

1. Plaintiff's Motion for Expedited Discovery (Dkt. #3) is DENIED.
2. Nothing in this Order precludes Plaintiff from renewing its motion once it can cure the deficiencies described above.

DATED this 26th day of December 2017.

RICARDO S. MARTINEZ
CHIEF UNITED STATES DISTRICT JUDGE